

































-  Secrets
-  ABAP
-  Apex
-  C
-  C++
-  CloudFormation
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  **HTML**
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML



# HTML static code analysis

Unique rules to find Bugs, Security Hotspots, and Code Smells in your HTML code

All rules 65 Bug 24 Security Hotspot 3 Code Smell 38

Tags

Search by name...

Table cells should reference their headers
Bug
Tables used for layout should not include semantic markup
Bug
Tables should have headers
Bug
"<html>" element should have a language attribute
Bug
<script>...</script> elements should not be nested
Bug
"<th>" tags should have "id" or "scope" attributes
Bug
"<title>" should be present in all pages
Bug
"<!DOCTYPE>" declarations should appear before "<html>" tags
Bug
Elements deprecated in HTML5 should not be used
Bug
HTML "<table>" should not be used for layout purposes
Code Smell
"aria-label" or "aria-labelledby" attributes should be used to differentiate similar elements
Code Smell
Videos should have subtitles
Code Smell

## Authorizing an opened window to access back to the originating window is security-sensitive

Analyze your code

Security Hotspot Minor cwe phishing owasp

A newly opened window having access back to the originating window could allow basic phishing attacks (the `window.opener` object is not `null` and thus `window.opener.location` can be set to a malicious website by the opened page).

For instance, an attacker can put a link (say: "`http://example.com/mylink`") on a popular website that changes, when opened, the original page to "`http://example.com/fake_login`". On "`http://example.com/fake_login`" there is a fake login page which could trick real users to enter their credentials.

### Ask Yourself Whether

- The application opens untrusted external URL.

There is a risk if you answered yes to this question.

### Recommended Secure Coding Practices

Use `noopener` to prevent untrusted pages from abusing `window.opener`.

Note: In Chrome 88+, Firefox 79+ or Safari 12.1+ `target=_blank` on anchors implies `rel=noopener` which make the protection enabled by default.

### Sensitive Code Example

```
<a href="http://example.com/dangerous" target="_blank">

<a href="{{variable}}" target="_blank"> <!-- Sensitive -->
```

### Compliant Solution

To prevent pages from abusing `window.opener`, use `rel=noopener` on `<a href=>` to force its value to be `null` on the opened pages.

```
<a href="http://petsocialnetwork.io" target="_blank" rel="noopener">
```











### Exceptions

No Issue will be raised when `href` contains a hardcoded relative url as there it has less chances of being vulnerable. An url is considered hardcoded and relative if it doesn't start with `http://` or `https://`, and if it does not contain any of the characters `{}$()[]`

```
<a href="internal.html" target="_blank" > <!-- Compliant -->
```

### See

- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- Reverse Tabnabbing
- MITRE, CWE-1022 - Use of Web Link to Untrusted Target with `window.opener` Access
- OWASP Top 10 2017 Category A6 - Security Misconfiguration

<b>Attributes deprecated in HTML5 should not be used</b>  Code Smell
<b>Sections of code should not be commented out</b>  Code Smell
<b>Track uses of "FIXME" tags</b>  Code Smell
<b>Meta tags should not be used to refresh or redirect</b>  Code Smell
<b>Links should not directly target images</b>  Code Smell
<b>"&lt;strong&gt;" and "&lt;em&gt;" tags should be used</b>  Bug
<b>"&lt;li&gt;" and "&lt;dt&gt;" item tags should be in "&lt;ul&gt;", "&lt;ol&gt;" or "&lt;dl&gt;" container tags</b>  Bug
<b>Server-side image maps ("ismap" attribute) should not be used</b>  Bug
<b>"&lt;frames&gt;" should have a "title" attribute</b>  Bug
<b>"&lt;fieldset&gt;" tags should contain a "&lt;legend&gt;"</b>  Bug
<b>Flash animations should be embedded</b>

- <https://mathiasbynens.github.io/rel-noopener/>

Available In:

